PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/06, 9/08

A1

(11) International Publication Number: **WO 95/26087**

(43) International Publication Date: 28 September 1995 (28.09.95)

(21) International Application Number: PCT/GB95/00660

(22) International Filing Date: 23 March 1995 (23.03.95)

(30) Priority Data:
9405766.8 23 March 1994 (23.03.94) GB

(71) Applicant *(for all designated States except US)*: CHANTILLEY CORPORATION LIMITED [GB/GB]; 28 Main Street, Mursley, Milton Keynes, Buckinghamshire MK17 0RT (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: HAWTHORNE, William, McMullan [GB/GB]; Kenmare, Bramerton Road, Surlingham, Norwich, Norfolk NR14 7DE (GB).

(74) Agent: EVANS, Huw, D., D.; Urquhart-Dykes & Lord, Three Trinity Court, 21-27 Newport Road, Cardiff CF2 1AA (GB).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: APPARATUS FOR GENERATING ENCRYPTION/DECRYPTION LOOK-UP TABLES USING A SESSION KEY

(57) Abstract

An encryption/decryption apparatus enables encrypted communication between two stations each incorporating such an apparatus. The apparatus is arranged to generate a set of look-up tables in accordance with a session key and temporarily store these tables in memory (18), and to convert each successive element (e.g. character) of a message to a code through use of the look-up tables. The session key can be changed as often as desired but the fresh set of look-up are created quickly each time; then the conversion process for each element of the message is carried out quickly yet maintaining a high level of security.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

APPARATUS FOR GENERATING ENCRYPTION/DECRYPTION LOOK-UP TABLES USING A SESSION KEY.

The present invention relates to arrangements for the automatic encryption and decryption of electronically transmitted messages, particularly in the fields of telephone, facsimile or computer data transmission for example.

The present invention is concerned with providing arrangements for encrypting and decrypting messages at high speeds yet maintaining a high level of security.

In accordance with this invention, there is provided an encryption/decryption apparatus to enable encrypted communication between two stations each incorporating such an apparatus, the apparatus being arranged to generate a set of look-up tables in accordance with a session key and temporarily store said tables in memory, and to convert each successive element of a message to a code through use of said look-up tables.

It will be appreciated that a fresh session key is used for each transmission or session: a fresh set of look-up tables is therefore generated at the start of each transmission or session. The session key can in fact be changed (and a new set of look-up tables consequently generated) at intervals during the course of each transmission.

The set of look-up tables can be generated quickly, and the procedure to encode each element (e.g. character, bit or block) of the message can be carried out quickly yet maintaining a high level of security.

Each element of the message may be converted to its code by addressing one of the look-up tables, the output of which is used to address another of the look-up tables, and so on. The conversion procedure may involve at least two look-up tables being addressed simultaneously and their outputs being combined (e.g. added together). At least one of the tables may comprise a pseudo random sequence, the terms (or entries) of which are read consecutively, the pointer returning to the first term when the last term of the table has been read: the pointer may start at any predetermined position of the sequence.

It will be appreciated that for encryption of a message by the sender and correct decryption by the recipient, both sender and recipient apparatus must use the same session key for each transmission (or part thereof), so that the two stations can generate corresponding look-up tables. Our International patent application PCT/GB94/02004 describes one arrangement in which a sender apparatus generates a session key and the same session key is recreated at the recipient.

Embodiments of this invention will now be described by way of examples only and with reference to the accompanying drawings, in which:

FIGURE 1 is a schematic block diagram of an encrypting/decrypting unit used at each sender/recipient station;

FIGURE 2 is a schematic flow diagram to explain the operation of one form of high speed cypher in accordance with the invention;

FIGURE 3 is a similar flow diagram to explain the operation of another form of high speed cypher in accordance with the invention;

FIGURE 4 is a worked example of an encryption procedure performed by an apparatus in accordance with the invention; and

FIGURE 5 is a worked example of another encryption procedure performed by an apparatus in accordance with the invention.

Referring to Figure 1, there is shown an encryption/decryption unit in accordance with this invention, in simplified diagrammatic form. Typically the unit will form part of a communications machine (e.g. facsimile machine). The unit includes an external port 10 for transmitting encrypted data to, and receiving encrypted data from, a corresponding unit at another station, with which it is desired to communicate. The unit also includes a port 12 for the flow of data to and from local host equipment. The unit further includes a microprocessor 14 having a program memory 16 and a memory 18 for temporarily holding look-up tables which are used for encrypting data to be transmitted via the external port 10, and for decrypting data received via the external port 10.

For each fresh transmission (or session) between the

unit and a corresponding unit at another station, a new set of look-up tables is generated and programmed into the memory 18 of the two units. Each new set of look-up tables is generated in accordance with a new, random session key: the program memory 16 of the two communicating units stores the same algorithm for generating (and subsequently using) the look-up tables, so that both units generate the same look-up tables from the same session key. One unit acts as sender and generates the random session key and sends this in encrypted form to the other (or recipient) unit: the session key may be generated at the sender, and recreated at the recipient, in the manner described in our International patent application PCT/GB94/02004. As previously noted, the session key can be changed at intervals within each transmission (or session).

Once each new set of look-up tables has been created, from the new session key, at the sender and recipient units, the encrypted transmission of data can proceed: thus, a plain message received at port 12 of the sender unit is encrypted, under control of the microprocessor 14 and using the look-up tables, and then transmitted via the data port 10; the recipient unit correspondingly receives the encrypted message and decrypts it.

The look-up tables are preferably of the types T,IT, D, ID or PR, as will now be described. Each table may have more than 4000 entries, but the essential character of the different types of table can be exemplified as follows using 10 entries only.

A transposition table (Type T) is a table in which numbers or characters are in a different order from the original, for example as follows:

Original order	0 1 2 3 4 5 6 7 8 9
T Table	4 3 5 7 1 0 8 6 9 2

The inverse transposition table (Type ID) is the inverse of the above in that it restores the original order when it is applied to the T table:

	0 1 2 3 4 5 6 7 8 9
IT Table	5 4 9 1 0 2 7 3 6 8

The displacement table (Type D) is derived from the transposition table and gives the positive displacement of each

entry in the transposition table from its original position:

Original order	0	1	2	3	4	5	6	7	8	9
T Table	4	3	5	7	1	0	8	6	9	2
D Table	4	2	3	4	7	5	2	9	1	3

The inverse displacement table (Type IT) is the displacement table corresponding to the inverse transposition table.

A pseudo-random table (Type PR) is composed of pseudo-randomly generated numbers in a specified domain:

Domain	0	1	2	3	4	5	6	7	8	9
PR Table	1	4	4	8	7	6	3	2	8	5

In a PR table, numbers within the domain may be omitted and others duplicated because the choice of entry at any part of the table does not depend on the choice of previous entries.

In the example shown in Figure 2, each successive character of the message to be encrypted is referred to a first look-up table which may be of any type previously described. The output of the first look-up table addresses the second look-up table and the output of the second addresses the third and so on. In this way, a succession of elements (e.g. character, bit or block) in the input message is converted to a corresponding succession of encrypted outputs from the final look-up table, for transmission from the sender to the recipient.

The look-up tables of the set may be used in different order on different transmissions as a means of increasing the complexity of the cypher: alternatively, each element in the main message may be converted by addressing two or more look-up tables simultaneously and combining (e.g. adding together) their outputs, as shown in Figure 3.

In the art of computer programming, reading a look-up table requires fewer steps than the multiplication and division steps usually carried out in element-by-element encryption, so that, once a set of tables has been generated, an algorithm largely based on reading tables permits rapid encryption. The decryption at the receiver is carried out in a similar manner, i.e. by each encrypted element of the received message being converted, by a corresponding arrangement of look-up tables, to the original element itself.

Figure 4 shows an example using a single T table and a single PR table. In this example, A = 0, B = 1, ... Z = 25, and all additions are modulo 26. After each character of the message is transposed by the transposition table, the next successive term of the PR table is added to provide the encryption of the original character.

Figure 5 shows an example using two D tables. However, the first table (D1) makes one rotary shift (i.e. the lower or output line shifts one step to the left) per character of the message: similarly, the second table (D2) makes one rotary shift per 26 characters of the message. Thus, for each character, the input and output of the first table (D1) are added together; this result is used to address the second table (D2) and is added together with the corresponding output of the second table (D2).

The session key may typically comprise a numerical decimal-digit number, for example up to 12 digits long. Many ways are known for generating a PR table from such a session key. Any convenient way may be used to generate a transposition table from such a session key, and one example will be explained with reference to the following table.

	0	1	2	3	4	5	6	7	8	9
4	4	1	2	3	0	5	6	7	8	9
1	4	1	2	3	0	5	6	7	8	9
3	4	1	3	2	0	5	6	7	8	9
6	4	1	3	6	0	5	2	7	8	9
0	0	1	3	6	4	5	2	7	8	9
1	0	5	3	6	4	1	2	7	8	9
4	0	5	3	6	2	1	4	7	8	9
0	7	5	3	6	2	1	4	0	8	9
6	7	5	3	6	2	1	8	0	4	9
0	9	5	3	6	2	1	8	0	4	7

The session key is set out in the vertical column at the extreme right hand side of the table. The successive terms of the session key (starting at the top of the column) are used in successive steps to change the original order (0, 1 ..... 9) given in the top row, to the T table given in the bottom

row. In the first step, the term "4" of the session key dictates that, in the initial row, the term in column 4 is exchanged with the term in column 0 (all other terms in the second row remain as in the first row). In the second step, the term "1" of the session key dictates that the term in column 1 is exchanged with the term in column 1 (with no net change in this case). In the third step, the term "3" of the session key dictates that the term in column 3 is exchanged with the term in column 2. The procedure progresses in this manner until, in the final step, the term "0" of the session key dictates that the term in column 0 is exchanged with the term in the final column. Having thus produced the T table, a D table can be generated, each of its terms being the displacement of the T table term from its corresponding original term.

CLAIMS

1) An encryption/decryption apparatus to enable encrypted communication between two stations each incorporating such an apparatus, the apparatus being arranged to generate a set of look-up tables in accordance with a session key and temporarily store said tables in memory, and to convert each successive element of a message to a code through use of said look-up tables.

2) An apparatus as claimed in claim 1, arranged for use of a fresh said session key at intervals during the course of each transmission.

3) An apparatus as claimed in claim 1 or 2, arranged to convert each element of the message to its said code by a procedure which comprises addressing one of the look-up tables and using the output of that table to address another of the look-up tables.

4) An apparatus as claimed in claim 1 or 2, arranged to convert each element of the message to its said code by a procedure which comprises addressing at least two of the look-up tables simultaneously and combining their outputs.

5) An apparatus as claimed in any preceding claim, in which at least one of the look-up tables comprises a transposition table.

6) An apparatus as claimed in any preceding claim, in which at least one of the look-up tables comprises a displacement table.

7) An apparatus as claimed in any preceding claim, in which at least one of the look-up tables comprises a sequence the entries of which are read consecutively.

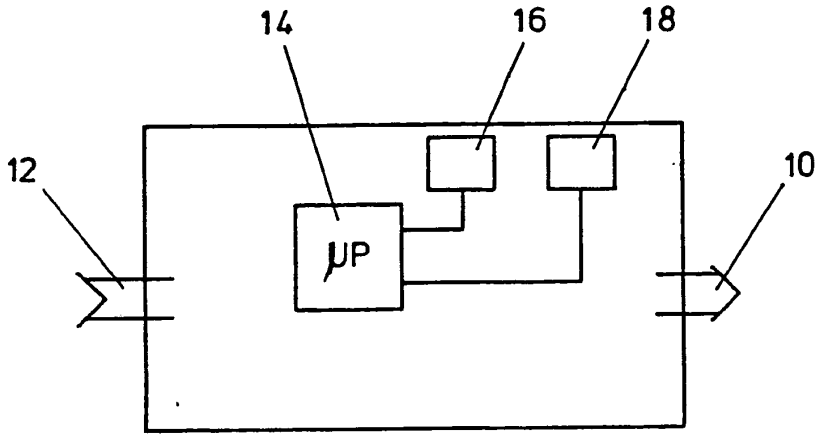

FIG. 1

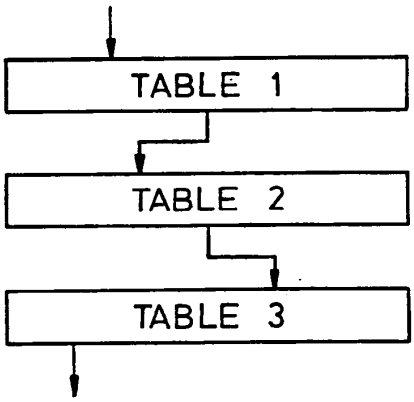

FIG. 2

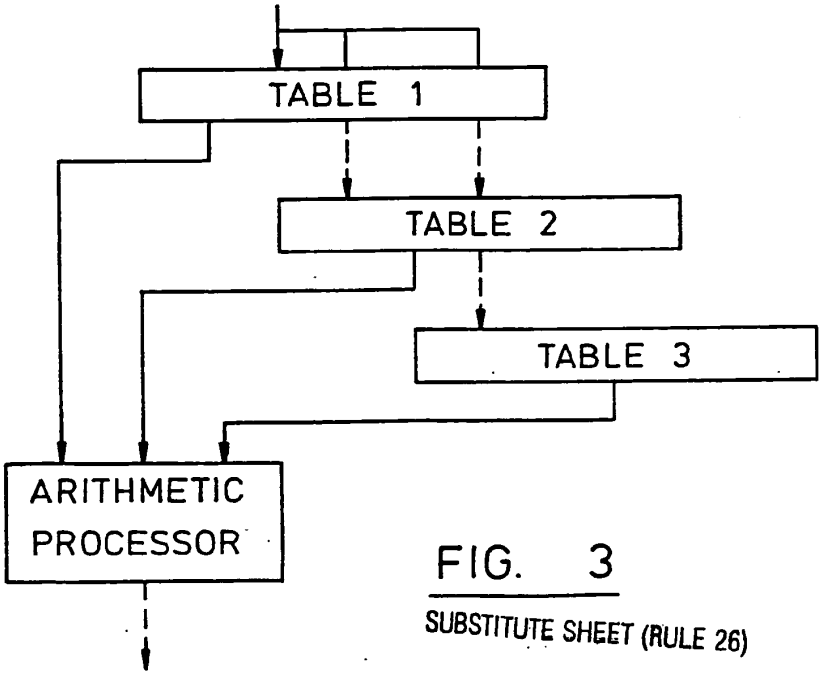

FIG. 3

FIG. 4

Transposition (T) table:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
7	17	19	23	14	12	21	24	13	20	11	6	18	4	16	25	1	9	15	0	22	10	3	5	2	8

Pseudo-random (PR) table:

18 13 15 7 7 20 0 19 21 18 1 10 22 20 9 25 22 1 24 9.....

Message:	M	E	X	I	C	A	N	B	A	N	K	S	A	T	R	I	S	K
	12	4	23	8	2	0	13	1	0	13	10	18	0	19	17	8	18	10

Transposition:	18	14	5	13	19	7	4	17	7	4	11	15	7	0	9	13	15	11
PR:	18	13	15	7	7	20	0	19	21	18	1	10	22	20	9	25	22	1.....
Addition of PR:	10	1	20	20	0	1	4	10	2	22	12	25	3	20	18	12	11	12
Crypt:	K	B	U	U	A	B	E	K	C	W	M	Z	D	U	S	M	L	M

FIG. 5

Displacement table D1:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
16	17	20	10	7	15	17	5	11	1	21	6	17	2	10	11	18	23	7	2	15	7	8	4	9	7

Displacement table D2:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
18	21	1	8	10	13	14	24	8	15	0	17	21	22	25	2	14	15	3	7	3	4	23	15	3	16

Message:	M	E	X	I	C	A	N	B	A	N	K	S	A	T	R	I	S	K
A=0.....Z=25:	12	4	23	8	2	0	13	1	0	13	10	18	0	19	17	8	18	10
Output from D1:	17	15	7	6	17	15	2	11	11	8	15	10	17	17	15	4	11	17
Add output:	3	19	4	14	19	15	15	12	11	21	25	2	17	10	6	12	3	1
Output from D2:	8	7	10	25	7	2	2	21	17	4	16	1	15	0	14	21	8	21
Add output:	11	0	14	13	0	17	17	7	2	25	15	3	6	10	20	7	11	22
Crypt A=0....Z=25:	L	A	O	N	A	R	R	H	C	Z	P	D	G	K	U	H	L	W

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/GB 95/00660

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/06 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,91 03113 (CRYPTECH) 7 March 1991 see page 10, line 1 - page 11, line 15 see page 12, line 30 - page 14, line 32 see page 15, line 18 - page 16, line 33 see figure 2	1,5,7
X	US,A,4 776 011 (BUSBY) 4 October 1988 see column 1, line 31 - column 2, line 43 see column 3, line 52 - column 4, line 24 see claim 1 see figures 1,2	1,7
X	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 22, no. 2, July 1979 NEW YORK US, pages 629-631, C.H.MEYER & W.L.TUCHMAN 'ESTABLISHMENT OF USER KEYS IN A MULTI-USER NETWORK' * the whole document *	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July 1995	24.07.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lydon, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/GB 95/00660

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9103113	07-03-91	US-A-	5003596	26-03-91
		AU-B-	635466	18-03-93
		AU-A-	6043190	03-04-91
		CA-A-	2064769	18-02-91
		EP-A-	0489742	17-06-92
		JP-T-	5501925	08-04-93
US-A-4776011	04-10-88	JP-B-	7023984	15-03-95
		JP-A-	60121486	28-06-85